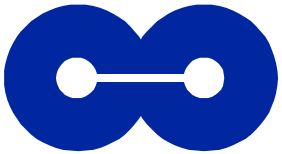


CYGNACOM SOLUTIONS

CygnaCom's Role in the Federal Bridge CA Demonstration

Certificate Path Development, Pilot Bridge CA, and S/MIME v3 Email client

Peter M. Hesse
pmhesse@cygnacom.com

Technology Solutions for Government and Business

Introduction

- **CygnaCom has developed three pieces of software that will be utilized in the Federal Bridge CA demonstration, scheduled for 9/99.**
- **Certificate Path Development Library (CPL)**
- **Pilot Federal Bridge CA**
- **S/MIME V3 Email Client**

CYGNACOM SOLUTIONS

Certificate Path Development Library (CPL)

- **The Certificate Path Development library constructs certificate paths in hierarchical or non-hierarchical certificate graphs**
- **It has a number of advantages over existing implementations**
  - Utilizes crossCertificatePair
  - Performs loop detection
  - Caches developed certificate paths
  - Contains many optimizations to help find the best path first

CYGNACOM SOLUTIONS

Certificate Path Development Library (CPL) (cont.)

- **Algorithm contains these matching rules**
  - Uses keyUsage and subjectKeyID as matching criteria (if present)
  - Ensures pathToName validates at every step
  - Skips invalid (expired) certificates
  - Allows specification of an acceptable list of algorithms
  - If initial-inhibit-policy mapping is TRUE, ensures intersection of certificatePolicies and initial-acceptable-policy-set ≠ 0

Certificate Path Development Library (CPL) (cont.)

- **Algorithm sorts certificates according to the following rules:**
  1) Certificates retrieved from the cACertificate attribute should have priority over certificates retrieved from the crossCertificate attribute
  2) Certificates in which algorithm used to sign the certificate matches the public key algorithm from the certificate should have priority
  3) Certificates that assert policies in the initial-acceptable-policy-set should have priority
  4) Certificates with fewer RDN elements in the Issuer DN should have priority
  5) Certificates match more RDNs between the issuer DN and relying party trust anchor DN should have priority
  6) Certificates that match more RDNs between the subject DN and the issuer DN should have priority
  7) Certificates with longer validity periods (furthest notAfter date) should have priority

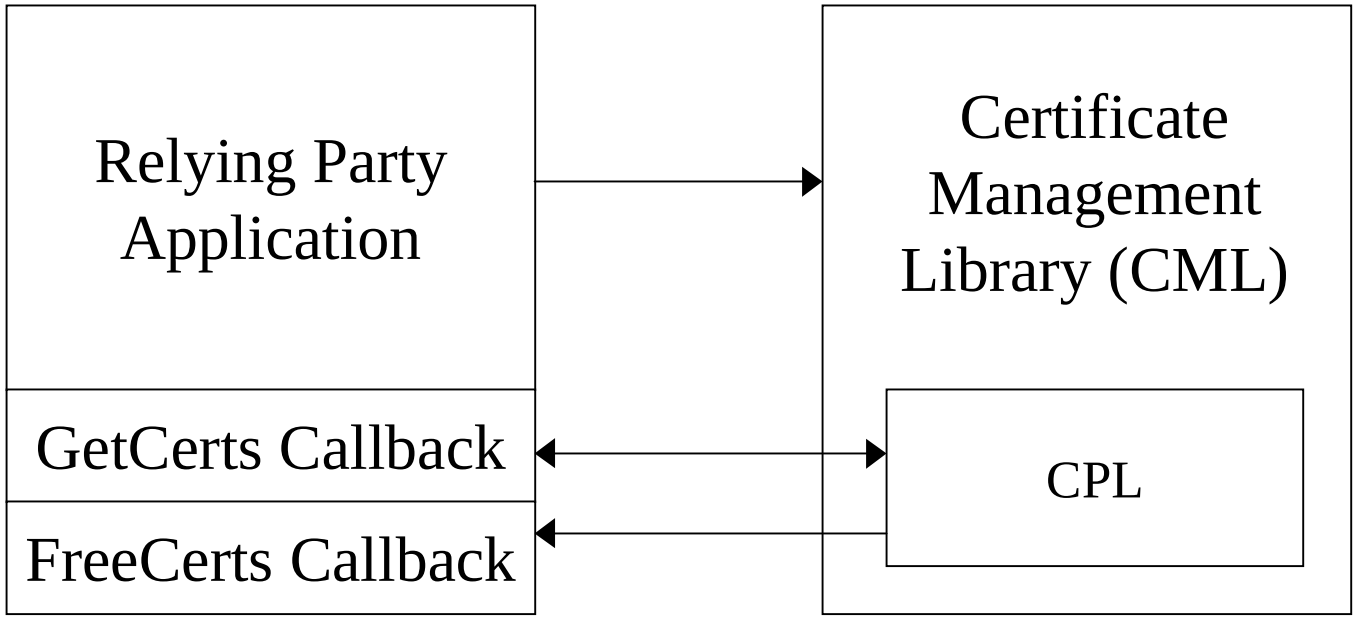
Certificate Path Development Library (CPL) (cont.)

- **CPL allows users to provide their own certificate/CRL caching and certificate/CRL retrieval**
  - This avoids reliance on any particular operating system or repository type (LDAP, X.500, Microsoft Active Directory)

- **CPL has been integrated into the NSA Certificate Management Library (CML) to replace its built-in path development capability**

CYGNACOM SOLUTIONS

Certificate Path Development Library (CPL) (cont.)



CYGNACOM SOLUTIONS

Certificate Path Development Library (CPL) (cont.)

- **We have requested NSA to allow us to release CPL as freeware**
  - To simplify one of the most complicated tasks in developing PKI software…
  - and to encourage thorough certificate path development
- **CPL was written in ANSI C++ to simplify portability to other platforms**
  - Currently available as a DLL for Windows 32-bit platforms (NT, Win95, Win98)

Pilot Bridge CA

- **The Pilot Bridge CA is based on the Minimum Interoperability Specification for PKI Components (MISPC) Reference Implementation, developed by CygnaCom for NIST**
- **Supports processing of Certificate Management Protocol (CMP)/Certificate Request Message Format (CRMF) cross-certificate requests, as well as manual cross-certification given a self-signed certificate**
- **Allows revocation of cross-certificates and generates CRLs periodically**

CYGNACOM SOLUTIONS

Pilot Bridge CA (cont.)

- **Fully-functional certificate authority, configured to issue cross-certificates**
- **Uses the Spyrus LYNKS crypto card**
- **Supports most X.509 certificate extensions**
- **Sends and receives CMP/CRMF requests/responses via email (SMTP/POP3)**
- **Creates crossCertificatePair objects and can post to an LDAP-compliant directory**

CYGNACOM SOLUTIONS

Pilot Bridge CA (cont.)

- **Extension Conflict Resolution Feature**
  - Two places to get extensions from:
    - CA Configuration
    - Certificate Request / Self-signed certificate input
  - Need to make sure CA Operator has some confidence on which will be chosen
    - Created wizard with one page for each supported extension
    - Any extension can be completely disallowed
    - Extensions may be configured to always choose CA-configured, requested, most restrictive, etc…

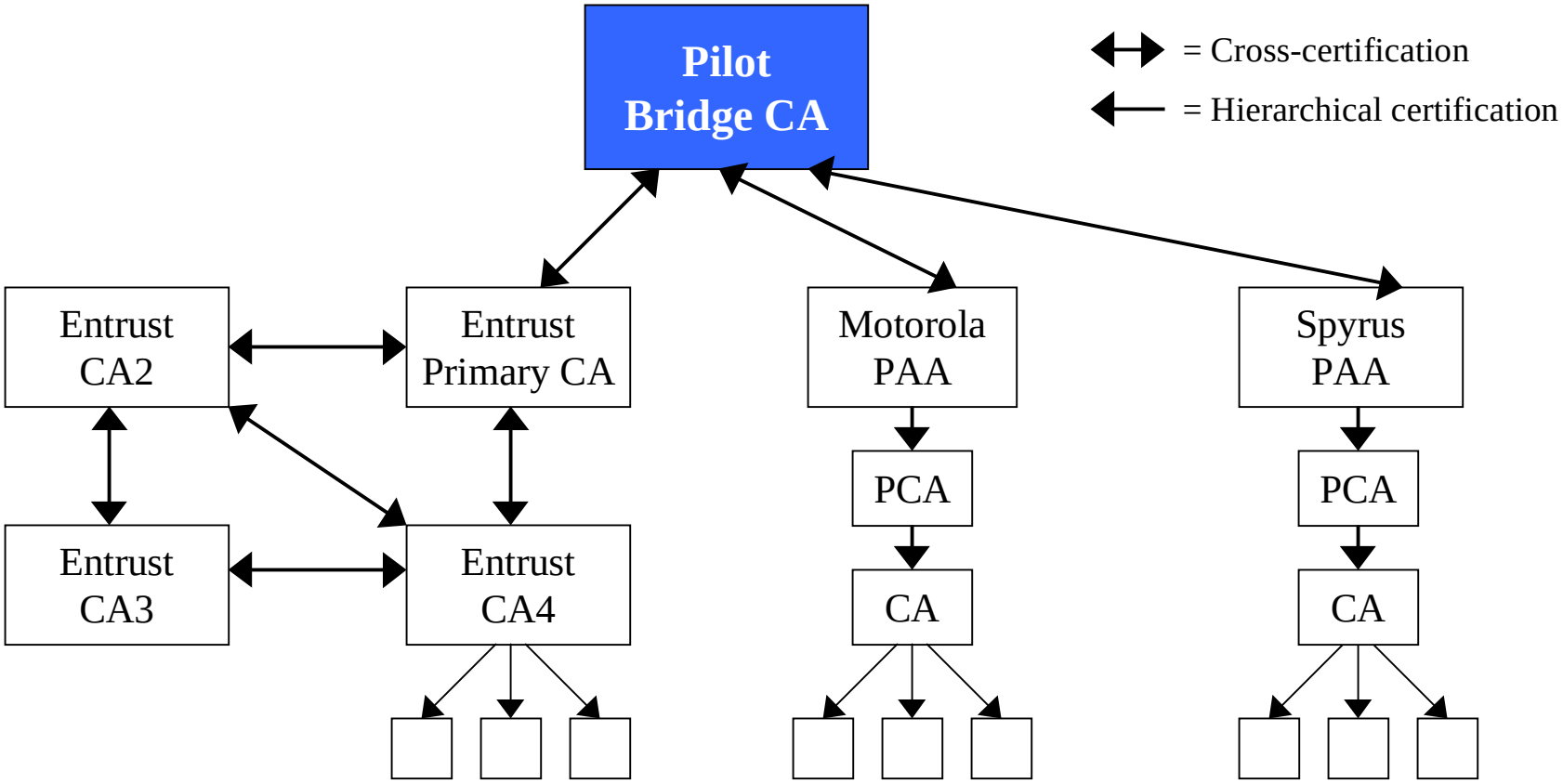
CYGNACOM SOLUTIONS

Pilot Bridge CA (cont.)

- **Developed for Windows NT**
- **Wizard-based configuration**
- **Simple, easy-to-understand interface**
  - Assumes basic PKI / X.509 knowledge from user
- **Up and running for 9/99 demonstration on July 1**

CYGNACOM SOLUTIONS

Pilot Bridge CA (cont.)



CYGNACOM SOLUTIONS

S/MIME V3 Client

- As part of the Federal Bridge CA Demonstration, CygnaCom has developed an S/MIME email application

- Rather than develop a custom interface that may be unfamiliar to users, we chose to develop it as a plug-in to Qualcomm's Eudora application

- Eudora provides the core email functionality (editing, MIME, networking) and we added hooks into the security libraries

CYGNACOM SOLUTIONS

S/MIME V3 Client (cont.)

- **Uses NSA Certificate Management Library (CML) for certificate/CRL parsing, caching, path validation**
  - Uses built-in CPL for building certificate paths
- **Uses VDA S/MIME Freeware Library (SFL) for S/MIME content parsing/verifying**
- **Uses Spyrus LYNKS crypto card for cryptographic operations**

S/MIME V3 Client Level of Effort

- **Start**
  - Little knowledge of S/MIME
  - No knowledge of Eudora Plugin API
  - No knowledge of S/MIME Freeware Library API
  - Little knowledge of Certificate Management Library
- **Finish**
  - Integrate all of above into fully functional client
- **Total**
  - Approximately 20W of effort
  - Most of effort was familiarization with interfaces, esp. SFL

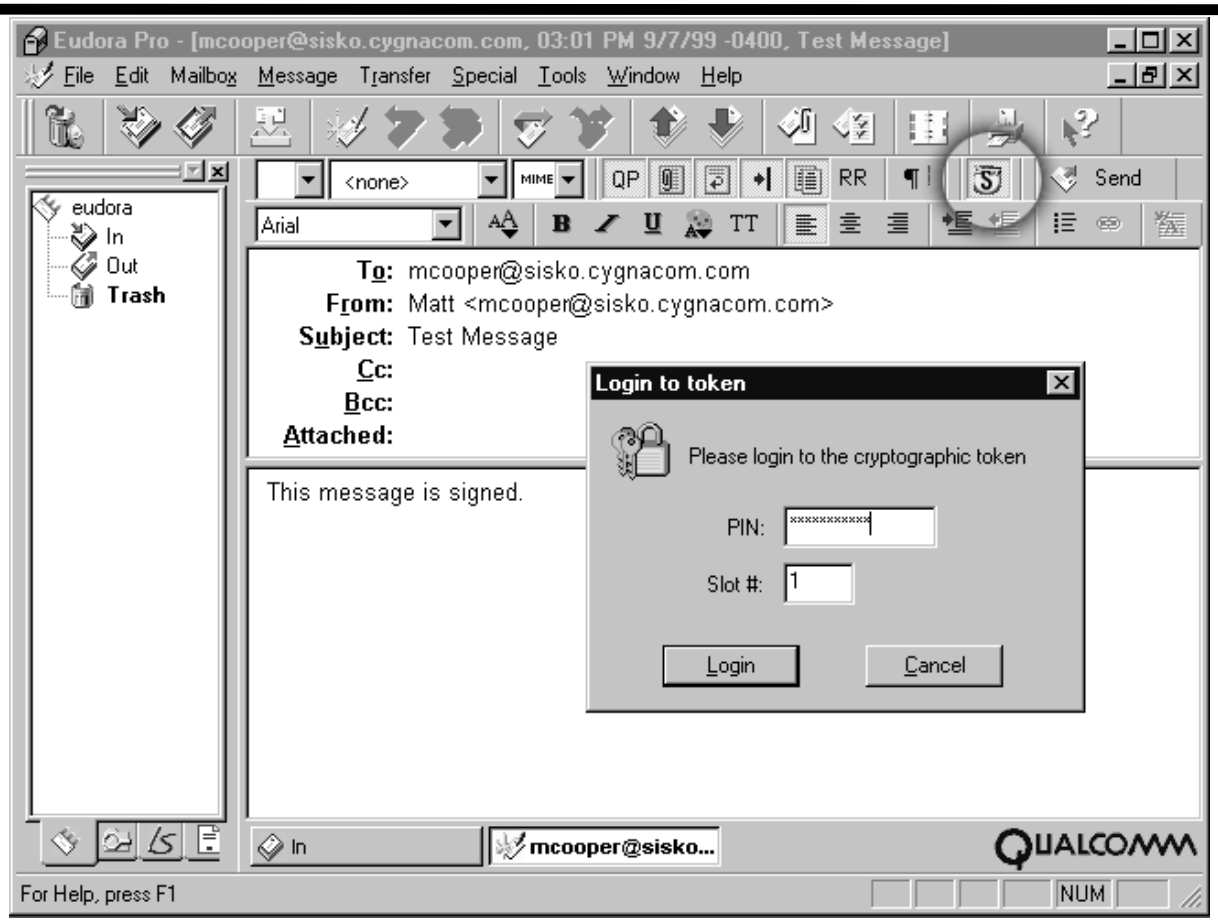
CYGNACOM SOLUTIONS

S/MIME V3 Client Level of Effort (cont.)

- **Further:**
  - Entrust contracted CygnaCom to develop client software similar to the NSA/SFL software but using Entrust FileToolkit™ instead of SFL
  - Already familiar with S/MIME
  - Previous experience with Entrust API
  - Already familiar with Eudora Plug-in API
- **Total Effort Estimated at less than 4 weeks**
  - Development underway and nearly complete
  - You *can* create a client in a reasonable time on a reasonable budget

CYGNACOM SOLUTIONS

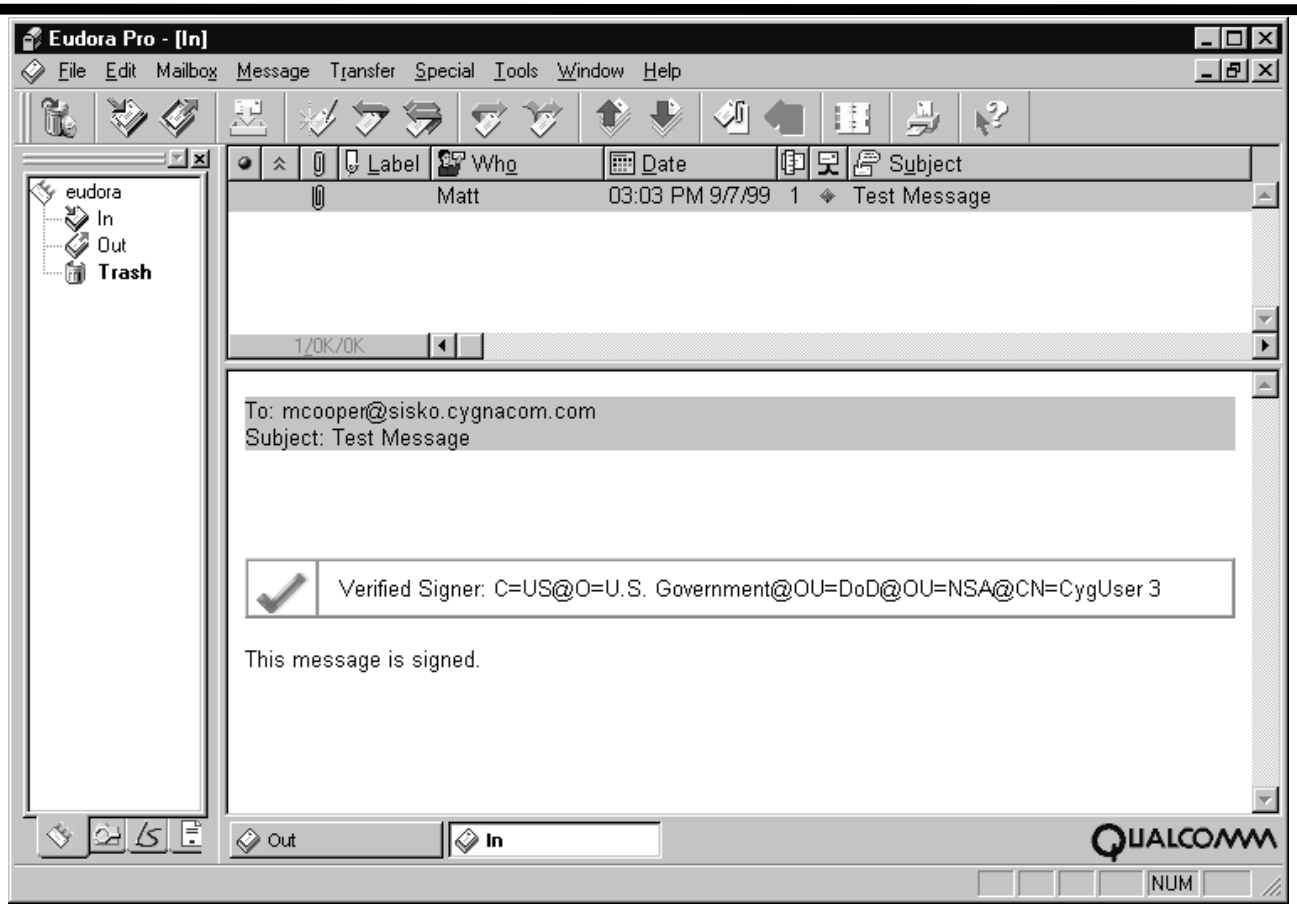
S/MIME V3 Client Screenshots
(Creating a signed message)



CYGNACOM SOLUTIONS

S/MIME V3 Client Screenshots

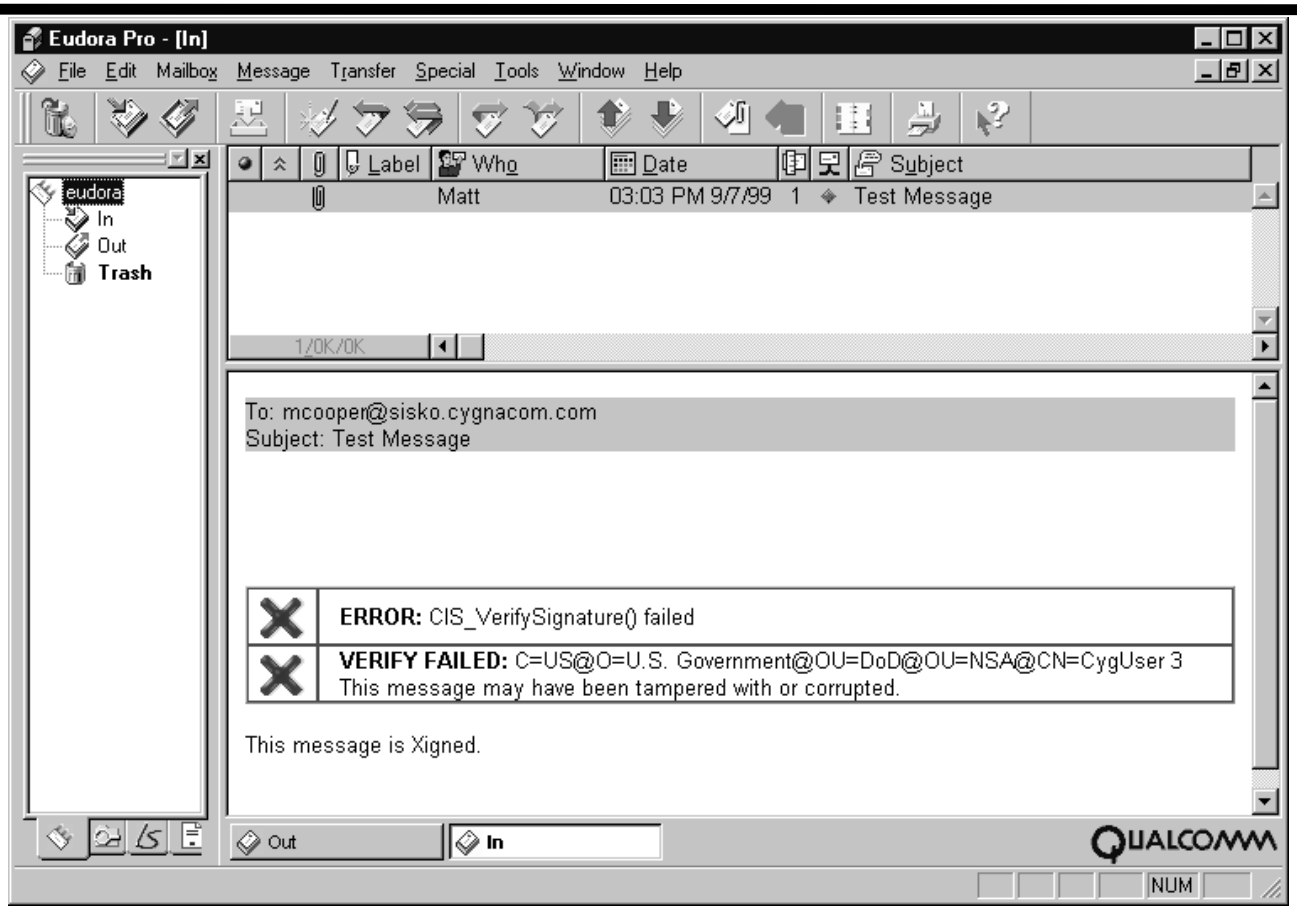
(Verifying a signed message)



CYGNACOM SOLUTIONS

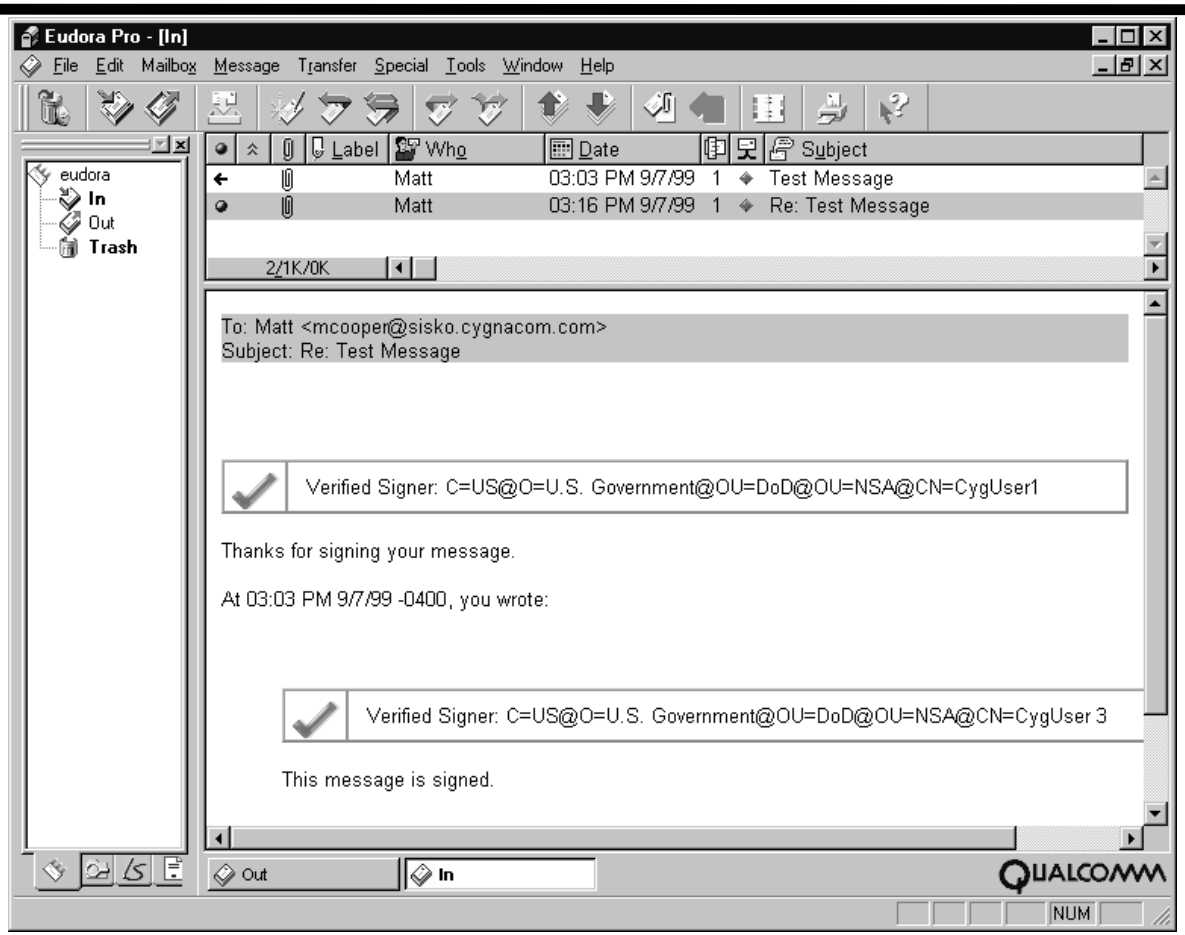
S/MIME V3 Client Screenshots

(Verifying a modified signed message)



CYGNACOM SOLUTIONS

S/MIME V3 Client Screenshots
(Verifying nested signed messages)



CYGNACOM SOLUTIONS

Questions?

- **If I cannot get to your question at this meeting, please contact me directly:**

Peter Hesse
Manager, Cryptographic Software Development
CygnaCom Solutions, Inc.
7927 Jones Branch Dr., Suite 100 West
McLean, VA 22102-3305
pmhesse@cygnacom.com
(703)848-0883 x212 (voice)
(703)848-0960 (fax)

CYGNACOM SOLUTIONS